U.S. Cyber Command Public Affairs
Cyber Guard 16

Cyber Guard 16 Fact Sheet

Cyber Guard 16 Overview:

Cyberspace and critical infrastructure operators and experts from more than 100 organizations, spanning government, academia, industry and allies, participated in the fifth annual Cyber Guard exercise, June 9-18th. U.S. Cyber Command, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) co-led the exercise, hosted by the Joint Staff in a state-of-the-art facility in Suffolk, VA designed to support a wide range of military tests and exercises. Participants exercised a whole-of-nation response to destructive cyber attacks against U.S. critical infrastructure. The exercise rehearsed operations designed to defend DoD Information Networks (DoDIN), and mitigate damage to Critical Infrastructure in a compromised cyber environment. The exercise aimed to refine information sharing and Defense Support to Civil Authorities processes and capabilities, strengthen partnerships within government, allies and the private sector, build and maintain DoD’s cyberspace capability and capacity, and continue efforts to build a Persistent Training Environment* (PTE) for cyberspace forces across DoD.

*PTE includes a closed exercise network, training event planning, management and assessment, a live expert opposing force and transport layer to enable distributed participation in the environment, and will be accessible to other U.S. government departments, allies and other partners, setting the foundation for whole-of-nation, full-spectrum cyberspace operations training.

Cyber Guard 16 Participants:

More than 800 individuals serving in various roles including 15 teams providing ‘over-the-shoulder’ training, assistance, and advising to private industry and DoD mission owners of Industrial Control Systems (ICS). Hands-on instruction and exercise scenarios were conducted on a closed classified network which emulates both DoD and non-DoD networks. Blue Team “friendly forces” worked to defend critical infrastructure networks and respond to a range of incidents, and a live, expert opposing force replicated a range of adversaries seeking to disrupt critical US infrastructure.

Cyber Guard History:

Cyber Guard is an evolving exercise, continually expanding to meet the demands of the Department of Defense and the nation. Cyber Guard 12 was developed to foster coordinated cyberspace incident responses between the Federal and state governments, exploring the National Guard’s potential as an enabler and “force multiplier” in the cyberspace domain. The exercise expanded in Cyber Guard 13 and 14 to include state and federal government and allied participation in an effort to develop and refine coordinated responses to cyber attack. Cyber Guard 15’s addition of private sector participation, coordinated through DHS, represented a shift from a whole-of-government to whole-of-nation approach to cybersecurity preparedness and response. Cyber Guard 16 built on previous lessons learned by expanding allied partner nation involvement for improvement of information sharing practices.

U.S. Cyber Command Mission:

- Provide mission assurance through the operation and defense of the Department of Defense information environment.
- Support the achievement of joint force commander objectives.
- When directed by the President, defend U.S. interests and infrastructure against cyber attack of critical consequence.